



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,863	01/05/2001	Kyle N. Patrick	CA920000037US1	3983
7590	06/28/2004		EXAMINER	
Jeanine S. Ray-Yarletts IBM Corp. Dept. T81/Bldg. 503-3 P.O.Box 12195 Research Triangle Park, NC 27709			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	2
DATE MAILED: 06/28/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/754,863	PATRICK, KYLE N. <i>[Signature]</i>
	Examiner	Art Unit
	Michael J Simitoski	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) Responsive to communication(s) filed on 05 January 2001.  
 2a) This action is FINAL.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) Claim(s) 1-14 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-14 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 05 January 2001 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_.  
 4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_.

## DETAILED ACTION

1. Claims 1-14 are pending.

### *Claim Rejections - 35 USC § 112*

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim is for a computer product, but it is unclear if the computer program product (such as a storage device) is to store the state object, as claimed, or if the claim is meant to convey that the client is to store the state object (line 29), as described in the specification.

### *Claim Rejections - 35 USC § 103*

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,134,592 to Montulli in view of "Assessing the Security of Your Web Applications" by Gaur in view of "Secure Cookies on the Web" by Park et al. (Park) in view of Applied Cryptography, Second Edition, by Schneier.

Regarding claims 1-5, Montulli discloses providing a client communicating a client request to said server/Web server to perform a server action/http request, said server responsive to receiving said client request, performing said server action/http request and creating a state object/cookie containing post-action state information, communicating said state object/cookie and a result of said server action/html document to said client, and storing said encrypted state object in said client memory, said client communicating a subsequent request to said server to perform a server action and said server receiving from said client said state object with said subsequent client request (col. 7, lines 33-50). Montulli lacks encrypting the cookie. However, Gaur teaches that to avoid a user gaining unauthorized access to personal information in cookies, one security measure is encrypting the cookie (page 3, §The security measures you can take are). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the cookie before sending it to the client and storing the encrypted cookie in the client memory. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized access to personal information, as taught by Gaur. As modified, Montulli lacks an asymmetric encryption method having a public key provided to said client said server and a private key provided to said server and encrypting said state object using said private key. However, Park teaches that an attacker can edit cookies and use them to impersonate the true owner of the cookie (page 39, §Providing Integrity). To prevent this, a server can issue the cookie with a digest to be later verified (that the cookie hasn't been modified) when the user presents the cookie (page 40-41, §Public-key-based solution). Park does not teach signing the whole key. However, Schneier teaches that one way to verify a document/cookie is to encrypt the document with the private key of a public key pair; the

document is verified when it is successfully decrypted using the public key (page 37, § Signing Documents with Public-Key Cryptography). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the state object/cookie using the private key of the server and to decrypt the received encrypted state object/cookie using the server public key. One of ordinary skill in the art would have been motivated to perform such a modification to prevent impersonation, as taught by Park (page 39, § Providing Integrity & page 40-41, § Public-key-based solution) and to verify the key, as taught by Schneier (page 37, § Signing Documents with Public-Key Cryptography).

Regarding claim 6, Montulli, as modified above, discloses using state information contained therein to perform the requested action (col. 7, lines 33-61), responsive to performing the requested action, replacing previous state information with new state information in said state object, encrypting said state object with said private key and sending said encrypted state object and a result of said server action to the client (col. 9, lines 38-63).

Regarding claims 7-10, the claims are substantially equivalent to claims 1-6. Therefore, claims 7-10 are rejected under similar rationale.

Regarding claims 11-14, as best understood, the claims are substantially equivalent to claims 1-6. Therefore, claims 11-14 are rejected under similar rationale.

### ***Double Patenting***

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686

Art Unit: 2134

F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1, 2, 4, 5, 7 & 11 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 2 of U.S. Patent No. 6,065,117 to White in view of “Secure Cookies on the Web” by Park et al. (Park) in view of Applied Cryptography, Second Edition, by Schneier. White discloses a method/system equivalent to the claimed method/system, but lacks using asymmetric cryptography. However, Park teaches that an attacker can edit cookies and use them to impersonate the true owner of the cookie (page 39, §Providing Integrity). To prevent this, a server can issue the cookie with a digest to be later verified (that the cookie hasn’t been modified) when the user presents the cookie (page 40-41, §Public-key-based solution). Park does not teach signing the whole key. However, Schneier teaches that one way to verify a document/cookie is to encrypt the document with the private key of a public key pair; the document is verified when it is successfully decrypted using the public key (page 37, §Signing Documents with Public-Key Cryptography). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the state object/cookie using the private key of the server and to decrypt the received encrypted state object/cookie using the server public key. One of ordinary skill in the art would have been motivated to perform such a modification to prevent impersonation, as taught by Park (page 39,

§Providing Integrity & page 40-41, §Public-key-based solution) and to verify the key, as taught by Schneier (page 37, §Signing Documents with Public-Key Cryptography).

### ***Conclusion***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. The Hartley, Kristol, Lin & Nelte are cited for teaching cookies and their uses.
- b. "Smart Certificates: Extending X.509 for Secure Attribute Services on the Web" is cited for teaching public key certificates containing attributes. The art is relevant in that it shows the transmission of certificates with attributes signed by a private key of a private/public key pair, to be verified by the public key of the pair.
- c. JP 411098134 A is cited for teaching the detection of alterations of cookies.
- d. The '359 reference is cited for teaching the use of cookies for authentication.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, DC 20231

**Or faxed to:**

Art Unit: 2134

(703)746-7239 (for formal communications intended for entry)

Or:

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS

June 15, 2004



GRIGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100